

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

TAMARA WILSON, individually and on
behalf of all others similarly
situated,

Plaintiff,

-against-

TRILLER, INC.,

Defendants.

21-cv-11228 (JSR)

OPINION AND ORDER

JED S. RAKOFF, U.S.D.J.

Plaintiff Tamara Wilson brings this class action against defendant Triller, Inc., alleging violations of state and federal law. Wilson claims that Triller's popular social media application - a competitor to TikTok that allows users to create, share and view short-form video content - collects and retains personally identifiable information about its users, including viewing history associated with a purportedly anonymized unique identifier assigned to each user, that Triller then unlawfully discloses to third parties, namely Facebook and Appsflyer. These third parties allegedly combine the disclosures with additional information at their disposal to identify users individually.

Before the Court is Triller's motion to dismiss Wilson's complaint pursuant to Fed. R. Civ. P. 12(b)(6). For the reasons that follow, Triller's motion is granted, with prejudice in part

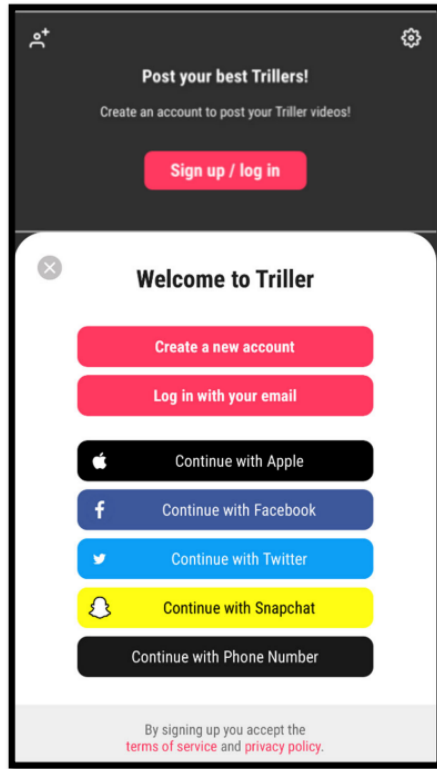
and without prejudice in part, and Wilson is granted leave to amend her complaint.

BACKGROUND

I. Factual Allegations

Defendant Triller, Inc., a Delaware corporation with its principal place of business in New York, “maintains and operates a popular social media application” (the “Triller App” or the “App”) “that allows users to view, share, upload, and create short videos.” ¶ 1.¹ “To post, comment, or like videos, or to watch certain content on the App, users must create a Triller account.” ¶¶ 8, 30. When creating an account, a user is presented with a screen, depicted below, that provides various ways to sign up for an account:

¹ Citations to ¶ __ are to Wilson’s complaint, ECF No. 1.



¶ 31. As seen in the screenshot, which was included in the complaint, at the bottom of the sign-up page is a disclosure regarding Triller's terms of use. This disclosure states that, "[b]y signing up you accept the terms of service [hyperlink] and privacy policy [hyperlink]." Id. Clicking on the hyperlinks or otherwise reviewing the terms of service or privacy policy documents (the "Terms") is not a mandatory step for using the app. Id.²

² If the user clicks "Create a new account," the user is prompted with another screen, featuring this same disclosure at the bottom, requesting that the user enter an email address, username, and password. ¶ 32. Alternatively, if the user chooses any of the "Continue with" options, no additional disclosure about the terms is displayed to the user. Id.

On the first page of Triller's privacy policy, which is incorporated into the complaint by reference, there is a header in large, bold print that states "Information We Collect and Receive." ECF No. 35-1 ("Privacy Policy") at 1. Under this header, the policy discloses that Triller collects "Personal Information," meaning "[i]nformation that could be directly associated with you, or used to contact or identify you, without the aid of additional information, including, without limitation information you provide us when you create an Account such as your name, age, date of birth, gender, address, email address, social media login details, telephone number, photograph"

Id. It also discloses that Triller collects "Usage Information," including:

(i) times and dates and the extent of your usage of the Platform . . . (iv) the User Accounts and/or User Content you view, like comment on, share, follow, message, add memes to, and otherwise interact with, as well as the foregoing that other Users do with respect to your Account and/or User Content; (v) usage history such as areas and pages within the Platform that you access or use and/or which buttons in the Platform you click on . . . (ix) other device and Platform access information such as your browser type, operating system, IP address, referring/exit pages, and other unique device identifiers

Id. at 2-3. The privacy policy also discloses that it may share the information collected from users with external parties "regarding traffic on the Platform, including pages viewed,

content interacted with, and actions taken by Users when visiting the Platform.” Id. at 8.

The terms of service provide that “[t]hese terms of service and all other terms and conditions or documents incorporated by reference herein, including, without limitation, our Privacy Policy[,] constitute a legally binding agreement between Company and each registered or unregistered end user” and “[b]y accessing and using” the App and/or creating an account, the user is “deemed to have read, accepted, executed and be bound by” the Terms. ECF No. 38-2 (“Terms of Service”) at 1. The terms further state that they are governed by the laws of the State of New York and include a “Limitation of Liability” clause providing that the user agrees not to hold the company or its affiliates liable for any damage, suits, claims, or controversies arising from use of the App. Id. at 21-22.

According to the complaint, Triller collects and shares users’ information with two of its third-party corporate affiliates, Facebook and Appsflyer. ¶ 38. Specifically, Triller allegedly assigns to each user a unique user identification number (“UID”), and every time a user visits the App, Triller transfers to its corporate affiliates certain information associated with the UID, including: (1) the user’s country, (2) the user’s time zone, (3) any videos the user has loaded, played or liked; (4) any user’s profile that he or she

has visited; and (4) certain of the user's device information. ¶¶ 42-59. Additionally, when a user visits his or her own profile, Triller allegedly pairs the UID with any data from the user's profile page, such as anything written in the "About Me" section, the URL of the photo chosen by the user as an avatar, and whether the user has a linked Instagram account (and, if so, the username for that account), a linked Snapchat account or an associated Soundcloud URL. ¶ 43.

Plaintiff Tamara Wilson, a citizen and resident of the State of Illinois, alleges that she downloaded the Triller App and created an account, which she used for approximately six months, one hour per day. ¶ 4. Wilson at no point uploaded or posted any videos using the app, but she viewed, "liked," and commented on videos, and sent messages to other viewers concerning their videos. ¶¶ 5-6. Wilson alleges that she does not recall seeing the Terms upon registering for an account with the App. ¶ 7.

II. Procedural Background

On December 31, 2021, Wilson filed suit against Triller alleging that Triller unlawfully shared her information with third parties and asserting claims for: (1) violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) violation of the Video Privacy Protection Act, 18 U.S.C. § 2710; (3) unjust

enrichment; and (4) violation of the Illinois Consumer Fraud Act, 815 ILCS §§ 505, et seq.

Wilson seeks to pursue her claims on behalf of a "Nationwide Class" defined as "[a]ll persons who reside in the United States who used the Triller App," and two alternative subclasses: (1) the "Multistate Consumer Protection Class" defined as "[a]ll persons who reside in Illinois or any state with materially similar consumer protection laws who used the Triller App" and (2) the "Illinois Subclass" defined as, "[a]ll persons who reside in Illinois and used the Triller App to view and/or create one or more videos." ¶ 84. The complaint seeks damages, restitution, disgorgement, and various forms of injunctive relief, as well as attorneys' fees and costs.

Triller filed the present motion to dismiss the complaint in its entirety on February 28, 2022. ECF No. 33. Following full briefing, oral argument was held on March 30, 2022.

LEGAL STANDARD

To survive a Rule 12(b)(6) motion to dismiss, a plaintiff must provide grounds upon which her claim rests through "factual allegations sufficient 'to raise a right to relief above the speculative level.'" ATSI Commc'ns, Inc. v. Shaar Fund, Ltd., 493 F.3d 87, 98 (2d Cir. 2007) (quoting Bell Atl. Corp. v.

Twombly, 550 U.S. 544, 555 (2007)).³ To do so, the complaint must allege "enough facts to state a claim to relief that is plausible on its face." Starr v. Sony BMG Music Entm't, 592 F.3d 314, 321 (2d Cir. 2010) (quoting Twombly, 550 U.S. at 570). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). In applying this standard, the Court accepts as true all well-pled factual allegations, but does not credit "mere conclusory statements" or "[t]hreadbare recitals of the elements of a cause of action." Id. In deciding a motion pursuant to Rule 12(b)(6), the Court may consider documents incorporated by reference and materials "integral" to the complaint. Sira v. Morton, 380 F.3d 57, 67 (2d Cir. 2004).

DISCUSSION

I. Computer Fraud and Abuse Act

Wilson's first cause of action asserts liability under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. The CFAA makes it illegal for an individual to "intentionally access[] a computer without authorization or [to] exceed[]

³ Unless otherwise indicated, in quoting cases all internal quotation marks, alterations, emphases, footnotes, and citations are omitted.

authorized access, and thereby obtain[]: . . . (C) information from any protected computer.” 18 U.S.C. § 1030(a)(2)(C).

Although “initially enacted solely as a criminal statute to address the ‘then-novel problem of computer hacking,’” Fischkoff v. Iovance Biotherapeutics, Inc., 339 F. Supp. 3d 408, 418 (S.D.N.Y. 2018) (quoting Hancock v. Cty. of Rensselaer, 882 F.3d 58, 63 (2d Cir. 2018)), the statute was later amended to provide a private civil cause of action allowing “[a]ny person who suffers damage or loss by reason of a violation of this section . . . against the violator” so long as the conduct involves one of a number of additional factors set out in § 1030(c)(4)(A), see 18 U.S.C. § 1030(g).

Triller contends that Wilson fails to state a claim under the CFAA both because she has not pled facts showing that Triller exceeded its authorization to access her device and because she has not adequately alleged damages cognizable under the statute. Because the Court agrees that Wilson has failed to plead facts showing that Triller exceeded its authorized access within the meaning of the statute, the Court does not address the issue of whether Wilson has adequately alleged damages.

The CFAA defines “exceeds authorized access” to mean “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.” 18 U.S.C. § 1030(e)(6).

As the U.S. Supreme Court has recently explained, “an individual ‘exceeds authorized access’ when he accesses a computer with authorization but then obtains information located in particular areas of the computer – such as files, folders, or databases – that are off limits to him.” Van Buren v. United States, 141 S. Ct. 1648, 1662 (2021). On the other hand, individuals do not exceed their authorized access, as defined under the statute, when they “have improper motives for obtaining information that is otherwise available to them.” Id. at 1652.

Wilson alleges that Triller exceeded its authorized access by causing users “to download and install the App” to their mobile devices without informing users that the App contained code that went beyond what users expected the App to do,” by collecting and then disclosing the users’ information. ¶ 99. However, as Triller argues, even assuming that Wilson is not bound by the Terms and thus did not authorize Triller to collect and disclose her information, it is not the case that Triller collects this information by accessing parts of her device that she expected or understood to be “off limits” to Triller. Van Buren, 141 S. Ct. at 1662. Rather, Wilson merely alleges that Triller collects and then shares information about the manner in which she and other users interact through the App with Triller own servers. Thus, at most, Wilson alleges that Triller misused

the information it collected about her, which is insufficient to state a claim under the CFAA.

Wilson responds by likening the present case to Feldman v. Comp Trading, LLC, 2021 WL 930222 (E.D.N.Y. Mar. 11, 2021), a case in which a court denied a motion to dismiss a CFAA claim premised on the defendant's unauthorized access to the plaintiff's data hosted on a third-party cloud-based server. See id. at *6 (citing Prop. Rights Law Grp., P.C. v. Lynch, 2014 WL 2452803, at *14 (D. Haw. May 30, 2014)). But while a plaintiff's cloud account on a third-party server may conceivably be a "protected computer" within the meaning of the statute because of the way in which cloud accounts mimic local computer storage, see Prop. Rights Law Grp., 2014 WL 2452803, at *14, it does not follow that Triller improperly accessed Wilson's device when it collected information about how Wilson interacted with Triller's own servers. Thus, Wilson has not plausibly alleged that Triller exceeded its authorized access in violation of CFAA.

Accordingly, Wilson's CFAA claim is dismissed with prejudice.

II. Video Privacy Protection Act

Wilson's second cause of actions asserts violations of the Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710.

"Congress passed the [VPPA] in 1988 after the Washington City

Paper published Supreme Court nominee Robert Bork's video rental history." In re Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 278 (3d Cir. 2016) (citing Sen. Rep. No. 100-599, at 5 (1988)). "The paper had obtained (without Judge Bork's knowledge or consent) a list of the 146 films that the Bork family had rented from a Washington, D.C.-area video store." Id. Congress responded by passing that Act, with the goal, according to the Senate Report, of "preserv[ing] personal privacy with respect to the rental, purchase or delivery of video tapes or similar audio visual materials." Id. (quoting Sen. Rep. No. 100-599, at 1).

The VPPA prohibits a "video tape service provider" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider." 18 U.S.C. § 2710(b)(1). It also includes a separate provision imposing an obligation to "destroy personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected," see id. § 2710(e). The Act is, as various courts have noted, "not well drafted," Sterk v. Redbox Automated Retail, LLC, 672 F.3d 535, 538 (7th Cir. 2012), and it defines "personally identifiable information" ("PII") obliquely to "include[] information which identifies a person as having requested or obtained specific video materials or

services from a video tape service provider," 18 U.S.C. § 2710(a)(3).

Wilson alleges that Triller violated the VPPA by disclosing to Facebook and Appsflyer information regarding users' video watch history as well as other information that, according to the complaint, can be used by Facebook and Appsflyer to associate the watch history with a particular individual. Wilson also accuses Triller of violating the provision regarding the retention of PII. Triller argues for dismissal of Wilson's entire claim on the grounds that Wilson does not allege that Triller disclosed her PII. Triller also argues for dismissal of the retention-based allegations on the ground that the VPPA does not provide an independent right of action for failure to destroy user's information. The Court addresses each of these arguments in turn.

A. Personally Identifiable Information

The statute fails to provide a clear definition of PII, and, instead, as noted above, only defines such information as "includ[ing] information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3). As the Ninth Circuit has observed, because of the use of the word "include," PII "must include more information than that which, by itself, identifies an individual as having watched certain

videos," that is, PII must "cover[] some information that can be used to identify an individual." Eichenberger v. ESPN, Inc., 876 F.3d 979, 984 (9th Cir. 2017). This conclusion is reinforced by the statute's use of the word "identifiable," where "the suffix 'able' means 'capable of.'" Id.

The key question that follows then is "what information did Congress intend to cover as 'capable of' identifying an individual." Id. On this question, two approaches have emerged. On the one hand is the broader approach adopted by the First Circuit in Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482 (1st Cir. 2016). In Yershov, the First Circuit held that PII encompasses "information reasonably and foreseeably likely to reveal which . . . videos [a person] has obtained" to the third party to whom the information is disclosed. Id. at 486. Relying on this definition, the court concluded that the defendant, which operated the "USA Today Mobile App," disclosed PII when it shared with Adobe information about which videos the plaintiff-user watched on the smartphone application, along with "GPS coordinates of the device at the time the video was viewed" and "certain identifiers associated with the user's device." Id. at 484. In reaching this decision, the court explicitly relied on the allegation that the defendant knew Adobe would be able to use this information to identify the plaintiff with particularity because of vast

information the company collects about individuals for the purpose of creating "digital dossiers." Id. at 485-86.

On the other hand, the Third Circuit adopted a narrower approach in In re Nickelodeon, 827 F.3d 262. In that case, the court rejected the plaintiff's argument that the user's IP address, that is, the "number assigned to each device that is connected to the Internet that permits computer-specific online tracking," as well as certain other information about the user's browser and operating system setting, was PII, holding that PII only refers to "the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior." Id. at 282-83, 290. This narrower definition is consistent with the approach to PII that has been adopted by "[t]he majority of courts to address this issue," including at least one court in this District. Robinson v. Disney Online, 152 F. Supp. 3d 176, 180 (S.D.N.Y. 2015); see also Eichenberger, 876 F.3d at 985 (adopting In re Nickelodeon's definition).

Although acknowledging that the information disclosed by Triller was "anonymized" and thus did not itself identify Wilson or any other particular user, Wilson urges the Court to adopt the First Circuit's approach to PII and find that the shared data constituted PII because Triller knew that Facebook and Appsflyer would be able to combine it with other information so

as to deduce the true identity of the individual associated with the video watch data. See ECF No. 38 at 12. Triller, on the other hand, argues against adopting this approach, invoking the Robinson court's observation that "[i]f nearly any piece of information can, with enough effort on behalf of the recipient, be combined with other information so as to identify a person, then the scope of PII would be limitless." 152 F. Supp. 3d at 181.

As a matter of statutory interpretation, it appears that the narrower definition is the correct one. Under the approach set out by the First Circuit in Yershov, whether any particular set of information constitutes PII depends on the capabilities of the party or parties to which it is disclosed – that is, the scope of PII is recipient-dependent. However, the VPPA sets out requirements regarding the handling of PII that do not implicate the disclosure of such information to a recipient, including 18 U.S.C. § 2710(e), which imposes an obligation on any “person subject to [the Act]” to “destroy [PII] as soon as practicable.” It would make little sense for the scope of PII to be recipient-dependent where the conduct at issue does not involve disclosure to a third-party. Given the principle that “identical words and phrases within the same statute should normally be given the same meaning,” United States v. Tabb, 949 F.3d 81, 88 (2d Cir. 2020), it follows that the Third Circuit's definition of PII –

which does not make the scope of PII dependent on the specifics of the recipient of the disclosure, see In re Nickelodeon, 827 F.3d at 290 - applies throughout the Act.

Ultimately, however, the Court does not need to resolve this issue, because even accepting the broader approach endorsed by plaintiff, the complaint does not allege that Triller disclosed Wilson's PII. According to the complaint, Triller disclosed to the third parties Wilson's UID, her country, time zone, the videos she watched or otherwise engaged with, other profile's she viewed, as well as certain other information about her device. ¶¶ 42-59. But, according to the complaint, it is not this information alone that allows Facebook and Appsflyer to "easily associate UIDs with the individual user." ¶ 44. Rather, as alleged, in order to make this association, the third party must "pair" the UID with information from a user's Triller profile page, which may or may not contain various personal information about the user, such as any information included in the "About Me" page or a URL associated with a photograph of the user. See ¶¶ 43-44.

While the complaint alleges what sort of information could be included on a user's profile and then ultimately disclosed to the third parties, it contains no allegation as to what information was actually included on Wilson's profile nor how that information could be used by a third party to identify

Wilson. Indeed, the complaint lacks any allegation that would allow the Court to infer a “firm and readily foreseeable” connection between the information disclosed and Wilson’s identify, thus failing to state a claim under the VPPA even assuming the broader approach set out in Yershov. See 820 F.3d at 486.

As such, the complaint lacks well-pleaded factual allegations that “plausibly give rise to an entitlement to relief.” Iqbal, 556 U.S. at 679. Accordingly, the Court grants Triller’s motion to dismiss the VPPA claim in its entirety. However, because it is conceivable that Wilson can amend her complaint to rectify the above-noted deficiencies, the dismissal is without prejudice.⁴

⁴ Triller also argues that Wilson’s alleged injuries are “not within the zone-of-interest for a VPPA claim.” ECF No. 34 at 15. Subsection (b)(2) of the VPPA authorizes disclosures to third parties only with the consumer’s “informed, written consent” that is “distinct and separate” from any form setting out the consumer’s “legal and financial obligations,” and is either “given at the time disclosure is sought” or given in advance for a set period of time that cannot exceed two years. 18 U.S.C. § 2710(b)(2)(B). Triller concedes that the disclosures were included in the Terms, rather than a stand-alone document, and thus did not meet the requirements of the statute. However, Triller argues that any injury resulting from this “purely procedural violation is not within the zone-of-interests that Congress aimed to protect when it passed the VPPA.” ECF No. 34 at 14.

But this misapprehends the zone-of-interests doctrine. “Whether a plaintiff comes within the ‘zone of interests’ is an issue that requires us to determine, using traditional tools of

B. Destruction of Records

As already noted, in addition to alleging a violation of the VPPA's prohibition on disclosing PII, 18 U.S.C. § 2710(b), Wilson also alleges that Triller violated the separate provision of the Act imposing an obligation to "destroy [PII] as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected," id. § 2710(e); ¶¶ 116-17. Triller argues for dismissal of this claim on the ground that the Act does not provide a private right of action for violations of this provision.

Both the text and structure of the statute strongly support the conclusion that only § 2710(b) "can form the basis of liability." Daniel v. Cantrell, 375 F.3d 377, 384 (6th Cir. 2004); accord Sterk v. Redbox Automated Retail, LLC, 672 F.3d 535, 539 (7th Cir. 2012); Rodriguez v. Sony Computer Ent. Am., LLC, 801 F.3d 1045, 1053 (9th Cir. 2015).

First, as to the text, "only section (b) includes language relating to liability," Daniel, 375 F.3d at 384, providing that

statutory interpretation, whether a legislatively conferred cause of action encompasses a particular plaintiff's claim." Lexmark Int'l, Inc. v. Static Control Components, Inc., 572 U.S. 118, 127 (2014). Because it is clear from the statute that a "distinct and separate" disclosure form is required, there is no basis for Triller's assertion that Wilson's claim may be precluded simply because a lower, non-statutory disclosure bar has been met.

a "video tape service provider . . . shall be liable" for its breach, 18 U.S.C. § 2710(b)(1). In contrast, sections (d), which deals with receiving PII into evidence, and (e), which requires destroying the information, contain no such liability language. See id. § 2710(d), (e). And, as to § 2710(d), the rule of evidence, it would indeed be "odd to create a damages remedy for 'reciev[ing]' information in evidence in an official proceeding" particularly given that "judges are typically protected by absolute immunity." Sterk, 672 F.3d at 538.⁵

Second, as to structure, the placement of § 2710(c), which sets out the rules for bringing a "civil action" to enforce "this section," meaning § 2710, suggests that it only provides for enforcement of actions under § 2710(b): As the Seventh Circuit explained in Sterk, "[i]f (c) appeared after all the prohibitions, which is to say after (d) and (e) as well as (b), the natural inference would be that any violator of any of the prohibitions could be sued for damages. But instead (c) appears after just the first prohibition, the one in subsection (b), prohibiting disclosure," thus suggesting the civil action

⁵ Notably, § 2710(e)'s requirement that the PII be destroyed bears some similarity to another rule governing the retention of sensitive material during litigation - Federal Rule of Civil Procedure 26(b)(5)(B)'s requirement that inadvertently produced privileged materials be "promptly . . . destroy[ed]."

authorized by § 2710(c) is “limited to enforcing the prohibition of disclosure.” Id.⁶

Although Wilson concedes that she may not hold Triller liable for a violation of § 2710(e) through a § 2710(c) action, she nonetheless argues that she may seek injunctive and declaratory relief in connection to the alleged violation of § 2710(e). See ECF No. 38 at 14-15. In support of this position, Wilson relies on the basic principle that “absent the clearest command to the contrary from Congress, federal courts retain their equitable power to issue injunctions in suits over which they have jurisdiction.” Califano v. Yamasaki, 442 U.S. 682, 705 (1979).

However, equally fundamental is the principle that, “in the absence of statutory intent to create a private right and remedy, a cause of action does not exist and courts may not create one, no matter how desirable that might be as a policy

⁶ Although Title 18 of the U.S. Code includes a provision restricting reliance on a section’s placement within the code in the context of statutory interpretation, see 18 U.S.C. Front Matter at 5, this legislated canon of interpretation does not preclude drawing inferences where the relevant structure is reflected in the statute as it was enacted by Congress, as is the case here, see Pub.L. 100-618, § 2(a)(2), Nov. 5, 1988, 102 Stat. 3195. See Daniel B. Listwa, Comment, Uncovering the Codifier’s Canon: How Codification Informs Interpretation, 127 Yale L.J. 464, 476-86 (2017) (explaining the distinction between placement decisions attributable to Congress and those properly attributed to the staff of the Office of the Law Revision Counsel).

matter, or how compatible with the statute.” Alexander v. Sandoval, 532 U.S. 275, 286–87 (2001). Thus, because, as Wilson concedes, the statute does not provide a private cause of action to enforce violations of § 2710(e), the Court may not infer one. See Rodriguez, 801 F.3d at 1053 (rejecting plaintiff’s action for injunctive relief under 18 U.S.C. § 2710(e)).

Thus, while the Court grants Wilson leave to amend the complaint to address the deficiencies associated with the alleged violations of § 2710(b), any amendment of the complaint as to the assertions of a violation on § 2710(e) would be futile. Accordingly, Wilson’s claim under § 2710(e) is dismissed with prejudice.

III. Unjust Enrichment

Wilson’s third cause of action asserts a claim for unjust enrichment, seeking to recover “the benefits derived from [Triller’s allegedly] unlawful gathering and sharing of [its users’] data. ¶ 123. Triller argues that this cause of action should be dismissed because, “[u]nder New York law, a plaintiff cannot recover under an unjust enrichment theory where a contract governs the subject matter of the dispute.”

Himmelstein v. Matthew Bender & Co. Inc., 2018 WL 984850, at *6 (N.Y. Sup. Ct. N.Y. Cnty. Feb. 6, 2018) (citing Cox v. NAP

Constr. Co., Inc., 10 N.Y.3d 592, 607 (2008)).⁷ In particular, because the allegations that Triller sent Wilson's information to third parties without her specific consent relates to a matter explicitly addressed by the Terms, Triller argues her unjust enrichment claim is precluded.

Wilson responds that given her allegation that she was never aware of the Terms and her assertion that the Terms are essentially hidden on the sign-up page, "there is a bona fide dispute as to the existence of a contract, [and whether it] cover[s] the dispute in issue," precluding dismissal of her quasi-contract claim. Poller v. BioScrip, Inc., 974 F. Supp. 2d 204, 236 (S.D.N.Y. 2013).

The question of whether the Terms constitute an enforceable contract is one of state law. Under New York law,⁸ to prove the existence of an enforceable agreement, the moving party "must establish an offer, acceptance of the offer, consideration, mutual assent, and an intent to be bound." Kasowitz, Benson,

⁷ Where a valid contract is held to exist and the dispute falls within the four corners of that contract, the unjust enrichment claim is precluded even if the plaintiff has not brought a breach of contract claim. See, e.g., MMT Sales, Inc. v. Channel 53 Inc., WPGH Div., 1993 WL 541242, at *4 (S.D.N.Y. Dec. 27, 1993).

⁸ Both parties agree that New York law governs this question. "[W]here the parties have agreed to the application of the forum law, their consent concludes the choice of law inquiry." Cargo Partner AG v. Albatrans Inc., 207 F. Supp. 2d 86, 93 (S.D.N.Y. 2002), aff'd, 352 F.3d 41 (2d Cir. 2003).

Torres & Friedman, LLP v. Reade, 98 A.D.3d 403, 404 (1st Dep't 2012), aff'd, 20 N.Y.3d 1082 (2013). Mutual assent may be manifested "by word, act, or conduct which evinces the intention of the parties to contract." Minelli Constr. Co. v. Volmar Constr., Inc., 82 A.D.3d 720, 721 (N.Y. 2d Dep't 2011). As a result, a party will be found to be bound by a contract's terms when "he is on inquiry notice of them and assents to them through conduct that a reasonable person would understand to constitute assent." Starke v. SquareTrade, Inc., 913 F.3d 279, 289 (2d Cir. 2019).

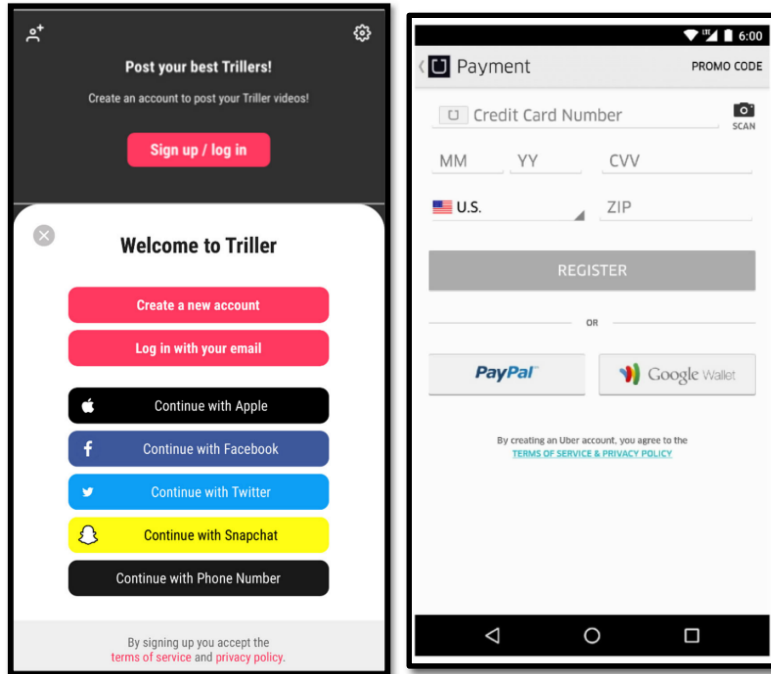
Whether an offeree is found to be on inquiry notice "often turns on whether contract terms were presented to the offeree in a clear and conspicuous way." Id. And in the context of "web-based contracts, we look to the design and content of the relevant interface to determine if the contract terms were presented to the offeree in way that would put her on inquiry notice of such terms." Id. For example, in Nicosia v. Amazon.com, Inc., 834 F.3d 220, 235-37 (2d Cir. 2016), the Second Circuit held that the plaintiff had plausibly pleaded that he was not bound by Amazon.com's conditions of use after he placed an online order, citing such facts as that the message alerting the user that placing an order constituted agreement to be bound by the conditions of use was not "bold, capitalized, or conspicuous in light of the whole webpage," and the page itself

contained “between fifteen and twenty-five links on the Order Page, and various text [was] displayed in at least four font sizes and six colors . . . alongside multiple buttons and promotional advertisements.”

In contrast, in Meyer v. Uber Techs., Inc., 868 F.3d 66, 81 (2d Cir. 2017), the Second Circuit enforced an arbitration provision contained in Uber’s “terms of service & privacy policy” that could be accessed by clicking on a link at the bottom of the registration screen of the Uber smartphone application.⁹ In reaching that decision, the court noted certain features of the interface’s layout, including that the screen was “uncluttered,” the “text, including the hyperlinks to the Terms and Conditions and Privacy Policy, appear[ed] directly below the buttons for registration”; “the dark print contrast[ed] with the bright white background, and the hyperlinks [were] in blue and underlined”; the “notice of the Terms of Service [was] provided simultaneously to enrollment”; and “[o]nce a user clicks through to the Terms of Service, the section heading (‘Dispute Resolution’) and the sentence waiving the user’s right to a jury trial on relevant claims [were] both bolded.” Id. at 78-79.

⁹ Although the Meyer Court applied California law, it noted that “New York and California apply substantially similar rules for determining whether the parties have mutually assented to a contract term.” 868 F.3d at 74,

Wilson argues that Triller fails to make the Terms sufficiently conspicuous on its sign-up page, noting that the hyperlinks appear in small text at the bottom of the page, below other “brightly colored login or sign-up buttons,” and that users are not required to either scroll through or acknowledge that they have read and understood the Terms. ¶ 76. However, as Triller notes, the presentation of the hyperlinks to the Terms was very similar to the presentation at issue in Meyers. As reflected in the side-by-side screenshots below, in both cases the hyperlinks appear directly below the buttons for registration in a smaller font and in a color that contrasts with the background; there is a warning that by creating an account with the respective platform, the user is agreeing to its respective terms; and the entire screen was visible at once, without there being a need to scroll beyond the page to find the terms. Compare ¶ 31, with Meyer, 868 F.3d at 78.



¶ 31; Meyer, 868 F.3d at add. A. And while there are certainly some differences, such as the color of the hyperlinked texts, given the strong similarities as to the relative conspicuousness of the disclosures regarding the terms of service and privacy policies, it follows that under Second Circuit precedent, Triller's Terms were sufficiently conspicuous to put the user on inquiry notice. As such, given the allegations of the complaint, an enforceable contract exists between Wilson and Triller.

Because the Court therefore finds that there is a valid contract between Wilson and Triller, see Terms of Service at 1, and because that contract governs the subject matter at issue here – that is, the collection and disclosure of Wilson's personal information associated with her use of the App, see

Privacy Policy at 1-3, it follows that Wilson's unjust enrichment claim is precluded as a matter of New York law.

Accordingly, the Court grants Triller's motion to dismiss the unjust enrichment claim. However, because it is conceivable that Wilson could amend her complaint to effectively call into question the validity of the contract purportedly created by the Terms, see, e.g., Metter v. Uber Techs., Inc., 2017 WL 1374579, at *3 (N.D. Cal. Apr. 17, 2017) (inquiry notice provided by the terms of service on Uber's registration page was deficient when obstructed by the user's "pop-up keypad"), the dismissal is without prejudice.¹⁰

IV. Illinois Consumer Fraud Act

Wilson's fourth cause of action asserts a violation of the Illinois Consumer Fraud Act ("ICFA"), 815 ILCS §§ 505, et seq. The ICFA prohibits "unfair or deceptive acts or practices, including . . . fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact" in the "conduct of any trade or commerce." Roppo v. Travelers Companies, 100 F. Supp. 3d 636, 650 (N.D. Ill. 2015) (quoting 815 ILCS § 505/2), aff'd sub nom. Sabrina Roppo v. Travelers Com. Ins. Co., 869 F.3d 568 (7th Cir. 2017).

¹⁰ Because the complaint is dismissed on other grounds, the Court declines to reach Triller's arguments regarding the applicability of the Term's limitation-of-liability clause.

Triller argues that Wilson's ICFA claim fails for several reasons, namely (1) the ICFA does not have extraterritorial effect and Wilson does not allege that the actions took place primarily and substantially in Illinois; (2) Wilson is not a "consumer" under the ICFA; (3) Wilson cannot allege she was deceived; and (4) Wilson has not adequately alleged damages.

"The ICFA does not have extraterritorial effect, and therefore applies only if the circumstances that relate to the disputed transaction occur primarily and substantially in Illinois." BCBSM, Inc. v. Walgreen Co., 512 F. Supp. 3d 837, 856 (N.D. Ill. 2021). Although no "bright-line test" is used to "determin[e] whether a transaction occurs within [the] state," "the Illinois Supreme Court considers" such factors as " (1) the claimant's residence; (2) the defendant's place of business; (3) the location of the relevant item that is the subject of the disputed transaction; (4) the location of the claimant's contacts with the defendant; (5) where the contracts at issue were executed; (6) the contract's choice of law provisions, if there are any; (7) where the allegedly deceptive statements were made; (8) where payments for services were to be sent; and (9) where complaints about the goods or services were to be directed." Id. (citing Serv. Corp. Int'l v. Stericycle, Inc., 2020 WL 43017, at *3-4 (N.D. Ill. Jan. 4, 2020)).

Here, Wilson's only allegation relating to Illinois is that she is a resident of that state. See ¶ 4. In contrast, other factors point outside the state, including that the defendant is a Delaware corporation with its principal place of business in New York, see ¶ 8, and that the Terms include a New York choice of law provision, see Terms at 22. Given the minimal contacts with Illinois alleged, there are insufficient connections to the state to hold that the ICFA applies. See Walker v. S.W.I.F.T. SCRL, 491 F. Supp. 2d 781, 795 (N.D. Ill. 2007) (finding "no substantial connection to Illinois," where "the only connection to the state of Illinois is that fact that plaintiff . . . is a resident of Illinois"). Wilson responds that the Court can infer that she also used the App in Illinois based on her residence, creating another factor in favor of finding this dispute falls within the statute's scope; however, a court may not "invent factual allegations that [the plaintiff] has not pled." Chavis v. Chappius, 618 F.3d 162, 170 (2d Cir. 2010).

Accordingly, Wilson's ICFA claim is dismissed. Because this deficiency may be rectified by amending the complaint, the dismissal is without prejudice.

CONCLUSION


For the foregoing reasons, the Court grants Triller's motion and dismisses Wilson's complaint with prejudice with regard to her claims under the CFAA and under § 2710(e) of the

VPPA, and without prejudice as to her other claims. Wilson is granted leave to amend the complaint. Any amended complaint must be filed by May 2, 2022. The Clerk of the Court is instructed to close document numbered 33 on the docket of this case.

SO ORDERED.

Dated: New York, NY

April 18, 2022


JED S. RAKOFF, U.S.D.J.